

237.7603

be incorporated in the contract, to ensure the continuation of these services in crisis situations. Contracting officers shall consult with a functional manager to assess the sufficiency of the contractor-provided written plan. Contractors will activate such plans only during periods of crisis, as authorized by the contracting officer, who does so at the direction of the appropriate functional commander or civilian equivalent.

(c) The contracting officer shall follow the procedures at PGI 207.105U(b)(20)(C) in preparing an acquisition plan.

237.7603 Solicitation provision and contract clause.

(a) Use the clause at 252.237-7023, Continuation of Essential Contractor Services in all solicitations and contracts for services that are in support of mission-essential functions.

(b) Use the provision at 252.237-7024, Notice of Continuation of Essential Contractor Services in all solicitations for services that include the clause 252.237-7023.

PART 239—ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 239.1—General

Sec.

239.101 Policy.

Subpart 239.70—Exchange or Sale of Information Technology

239.7001 Policy.

Subpart 239.71—Security and Privacy for Computer Systems

239.7100 Scope of subpart.

239.7101 Definition.

239.7102 Policy and responsibilities.

239.7102-1 General.

239.7102-2 Compromising emanations—TEMPEST or other standard.

239.7102-3 Information assurance contractor training and certification.

239.7103 Contract clauses.

Subpart 239.72—Standards

239.7201 Solicitation requirements.

Subpart 239.73 [Reserved]

48 CFR Ch. 2 (10-1-11 Edition)

Subpart 239.74—Telecommunications Services

239.7400 Scope.

239.7401 Definitions.

239.7402 Policy.

239.7403-239.7404 [Reserved]

239.7405 Delegated authority for telecommunications resources.

239.7406 Cost or pricing data and information other than cost or pricing data.

239.7407 Type of contract.

239.7408 Special construction.

239.7408-1 General.

239.7408-2 Applicability of construction labor standards for special construction.

239.7409 Special assembly.

239.7410 Cancellation and termination.

239.7411 Contract clauses.

AUTHORITY: 41 U.S.C. 421 and 48 CFR chapter 1.

SOURCE: 56 FR 36429, July 31, 1991, unless otherwise noted.

Subpart 239.1—General

239.101 Policy.

See Subpart 208.74 when acquiring commercial software or software maintenance. See 227.7202 for policy on the acquisition of commercial computer software and commercial computer software documentation.

[67 FR 65512, Oct. 25, 2002, as amended at 74 FR 34270, July 15, 2009]

Subpart 239.70—Exchange or Sale of Information Technology

239.7001 Policy.

Agencies shall follow the procedures in DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation, Chapter 9, Section C9.5, when considering the exchange or sale of Government-owned information technology.

[71 FR 39010, July 11, 2006]

Subpart 239.71—Security and Privacy for Computer Systems

SOURCE: 69 FR 35534, June 25, 2004, unless otherwise noted.

239.7100 Scope of subpart.

This subpart includes information assurance and Privacy Act considerations. Information assurance requirements are in addition to provisions

concerning protection of privacy of individuals (see FAR Subpart 24.1).

239.7101 Definition.

Information assurance, as used in this subpart, means measures that protect and defend information, that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed, and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

239.7102 Policy and responsibilities.

239.7102-1 General.

(a) Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes, to include—

- (1) The National Security Act;
- (2) The Clinger-Cohen Act;
- (3) National Security Telecommunications and Information Systems Security Policy No. 11;
- (4) Federal Information Processing Standards;
- (5) DoD Directive 8500.1, Information Assurance;
- (6) DoD Instruction 8500.2, Information Assurance Implementation;
- (7) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management; and
- (8) DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.

(b) For all acquisitions, the requiring activity is responsible for providing to the contracting officer—

- (1) Statements of work, specifications, or statements of objectives that meet information assurance requirements as specified in paragraph (a) of this subsection;
- (2) Inspection and acceptance contract requirements; and
- (3) A determination as to whether the information technology requires protection against compromising emanations.

[69 FR 35534, June 25, 2004, as amended at 73 FR 1829, Jan. 10, 2008; 75 FR 34946, June 21, 2010]

239.7102-2 Compromising emanations—TEMPEST or other standard.

For acquisitions requiring information assurance against compromising emanations, the requiring activity is responsible for providing to the contracting officer—

- (a) The required protections, *i.e.*, an established National TEMPEST standard (*e.g.*, NACSEM 5100, NACSIM 5100A) or a standard used by other authority;
- (b) The required identification markings to include markings for TEMPEST or other standard, certified equipment (especially if to be reused);
- (c) Inspection and acceptance requirements addressing the validation of compliance with TEMPEST or other standards; and
- (d) A date through which the accreditation is considered current for purposes of the proposed contract.

239.7102-3 Information assurance contractor training and certification.

(a) For acquisitions that include information assurance functional services for DoD information systems, or that require any appropriately cleared contractor personnel to access a DoD information system to perform contract duties, the requiring activity is responsible for providing to the contracting officer—(1) A list of information assurance functional responsibilities for DoD information systems by category (*e.g.*, technical or management) and level (*e.g.*, computing environment, network environment, or enclave); and

(2) The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information assurance functional responsibilities.

(b) After contract award, the requiring activity is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked.

(c) The responsibilities specified in paragraphs (a) and (b) of this section